EXHIBIT C

EMERALD™ TCP Statistical Analyzer 1998 Evaluation Results

The following are the unedited and annotated results from the EMERALD™ statistical analyzer (estat) TCP monitor on the two weeks of test data provided by MIT Lincoln Laboratory for the DARPA/ITO-sponsored 1998 Intrusion Detection Evaluation.

Contents:

Monitor Description

The EMERALD™ estat process statistically analyzes the data stream produced by the EMERALD™ TCP connection-event monitor (this monitor tracks the state of all TCP connection-oriented protocol elements, and generates summary events for each connection). The current TCP analysis is restricted to the externally initiated connections (i.e., external client accesses to a site's servers). Long-term profiles are built and maintained for each of the site's servers. Each connection-event contributes to the score of one or more statistically analyzed measures for a server. Each measure is individually scored against how well the short-term observations match the long-term profile for the server. A connection event is labeled anomalous when the aggregated score for all measures exceeds a statistically determined threshold for the server. The TCP monitor uses five measures:

1. conn_setup

   This measure monitors the connection establishment codes, which are one of the following (these names reflect those in the eresolv attack summary listing):

Setup Code	*Description*
OK	Connection setup successful (no errors).
RST-server	The server rejected the request.
RST-client	The client reset the connection instead of sending an acknowledgment (ACK) to complete the three-way handshake.
TO-server	The three-way handshake timed out waiting for the server to respond (with a SYN-ACK) to the connection request (a SYN) sent from the client.
TO-client	The three-way handshake timed out waiting for the client to respond (with an ACK) to the connection acknowledge (a SYN-ACK) sent from the server.

2. conn_setup_time

This measure tracks the round-trip time used to complete the three-way handshake (SYN, SYN-ACK, ACK). Although it is usually less than the setup time-out, it can be greater if the two parties keep sending packets to each other (sometimes the three-way handshake involves many more than just three packets).

3. server_port

This measure tracks server port numbers on connection attempts:

Ports	*Description*
< 1024	An IETF reserved (well known) port range
2049	nfsd: NFS server daemon
2766	listen: System V listener port
4045	lockd: NFS lock daemon/manager
6000-6010	X-server protocol port range
6112	dtspc: CDE subprocess control
7100	fs: Font server

If the port appears in (the range of) an entry in this list, the port number is retained as is. All other ports are assumed to be system-allocated ports whose values fall into distinct operating system-specific ranges. Thus, these "outlier" ports are hashed together by masking their off low-order 12 bits.

4. conn_shutdown

Shutdown Code	*Description*
OK	Normal connection close (no errors).
RST-server	The server reset the connection.
RST-client	The client reset the connection.
TO	The connection timed out (no traffic on this connection for at least 12 hours).
TO-close	A close (FIN) from one party was seen without a corresponding close from the other party within 5 minutes.

5. conn_duration

This measure tracks the total amount of time the connection stays open, regardless of how it terminated.

Attack Report Description

The EMERALD™ resolver groups together individual alert messages from the statistical analyzer. The first-level grouping is by internal host, labeled "Target" in attack reports and listed in dotted-ip notation. The resolver for this monitor has also been configured to treat the client (external) address as a secondary grouping key, labeled "clientAddr" in attack reports. An attack must accumulate at least ten anomalous events from the statistical analyzer before it is reported as an attack.

Each attack report begins with a target identifier, the score and/or the number of events contributing to the attack, the time (range) of the attack, and the client (external) address associated with the attack. From there, the attack report lists the relevant fields retained for that attack. Each field may have one or more values observed, and they are listed after the field name from most- to least-frequently observed. The time-oriented field values reported have been aggregated into appropriate bins (a nonlinear truncation of precision intended to give order-of-magnitude information). If the number of observations of a particular field value is different from the number of events in the attack, the actual number of observations is indicated in parenthesis following the display of the observed value. If there are too many fields to display, the most frequent few are displayed, followed by a summary histogram of the number of observations for each decreasing hit-rate range.

For example, the attack report

```
Target 172.16.114.50       28 events
  from 1998-07-21 11:35:00.000426 EDT to 1998-07-21 19:15:54.000103 EDT
  clientAddr:  135.8.60.182
  connSetup.score:  5.0
  connSetupTime.score:  3.5 (2)
  connShutdown.score:  5.0
  conn_setup:  RST-server (15)
  conn_setup_time:   0.000001000 (20)   0.000000000 (2)   2.000000000 (1)
  server_port:  http (27)  telnet (1)
```

indicates that the local host 172.16.114.50 saw 28 anomalous connection events from host 135.8.60.182 between 11:35 and 19:16 EDT on July 21, 1998. The connection setup measure's score was 5.0 for all 28 events, whereas the connection setup time measure's score was 3.5 for two of the events (and therefore below 3.0 for the other 26 -- thus connection setup time measure did not significantly contribute to the anomaly). The connection shutdown measure's score was also 5.0 for all 28 events. The connection setup code for 15 of the events was a server reset, indicating that the service(s) were off-line. We also see three (binned) observed values for connection setup times: 1.0e-6 (20 events), 0 (two events), and 2 (one event). Last, we see that 27 of the events were connections to the server's (host 172.16.114.50) http port, and one event was to its telnet port.

Each attack report contains fields identifying the observed individual measure scores for the events assigned to the attack (these will be field names of the form <measure-name>".score"). The score resolution reported here has been reduced to the nearest 0.5, and will be reported only when the score exceeds a minimum threshold of 3.0. This information helps identify how much each measure contributed to the aggregate attack score. Different attacks will affect the measures in different ways.

In addition to the measure scores, the observed values will be displayed for those event fields that significantly contributed to the measure's score. In some cases, a high score may be displayed without any corresponding field observations. This happens when a prior anomaly saturates the measure and the current observations, while bringing the score down, still maintain a high score.

The last item displayed in the attack report is the server's port, which is displayed regardless of its measure's contribution in order to facilitate identification of the affected service(s).

Test Description

The monitor's statistics were trained on eight days from the LL training dataset. The training days were specifically selected because they contained the fewest perturbations after known attacks (from the list-file) were removed (by removing all data from the specified time segments). In order to achieve adequate training, however, we had to run the eight-day dataset through the statistical analyzer five times for a total of 40 days of training (not all days contained data for all hosts -- the additional days were to train the less-frequently accessed hosts). We then made one final pass through the training data without any profile learning (to test how well the analyzer trained on the data it was given, and how well the dataset as a whole can be described by a fixed profile), and no attacks were detected.

Some sample training data score plots:

- pascal
- zeno
- marx

We ran each day from the LL test data separately, using the same starting profile (from the training data), to avoid having one day's results contaminate the others. The entire run of data through the statistical analyzer and resolver (58 days: 40 training, 8 training-check, and 10 test days) took approximately 47 minutes to complete.

1998 Evaluation Attack Reports

Summary:

Test Day	*Detections*	*False Alerts*
Week 1 Monday	0	0
Week 1 Tuesday	2	0
Week 1 Wednesday	0	0
Week 1 Thursday	0	0
Week 1 Friday	3	0
Week 2 Monday	3	0
Week 2 Tuesday	4	0
Week 2 Wednesday	2	0
Week 2 Thursday	4	0
Week 2 Friday	3	0
Totals	21	0

The EMERALD™ statistical analyzer TCP monitor was designed to detect large-scale changes in the relative volume of connection setup outcomes, as typically happens with SYN-flood (neptune) attacks, and we successfully detected all six such attacks in the LL dataset. In addition, we detected several attacks for which the monitor was not specifically designed because these denial-of-service attacks adversely affected the ability of the targeted host to create and/or maintain TCP connections. In some cases, this meant that we detected the side effects or consequences of the attack, rather than detecting the attack directly.

In addition, the test data often contain consecutive attacks with little or no intervening "normal" data (note: our monitor will only "reset" itself with intervening data, the mere passage of time is insufficient). Thus, we find that our detection rate is artificially high because an attack, which in isolation would not have sufficiently perturbed the statistics, piggy-backs on the residual effects of the prior attack.

Week 1 Monday:

There were no attacks detected for this day. Some sample test result score plots:

- pascal
- zeno
- marx

Week 1 Tuesday:

The following eight reports have identified that there was a problem with web (http) services on marx (172.16.114.50) beginning at 10:24:28 and continuing as late as 19:15:54. The first report actually identifies the culprit, and corresponds to the apache2 attack identification in the list file. We infer from the large number of reset-by-server connection codes that the attack did, in fact, cause at least the http service to crash, if not the entire host, and that this service was not promptly restored after the attack.

```
Target 172.16.114.50      188 events
  from 1998-07-21 10:24:28.000460 EDT to 1998-07-21 10:27:14.000908 EDT
  from source estat-TCP-monitor
  clientAddr:  207.181.92.211
  server_port:  http
  connSetup.score:  5.0
  connShutdown.score:  5.0
  conn_shutdown:  RST-server
  connSetupTime.score:  3.5
  conn_duration:  480.000000000 (180)  900.000000000 (7)

Target 172.16.114.50       28 events
  from 1998-07-21 11:35:00.000426 EDT to 1998-07-21 19:15:54.000103 EDT
  from source estat-TCP-monitor
  clientAddr:  135.8.60.182
  server_port:  http (27)  telnet (1)
  connSetup.score:  5.0
  conn_setup:  RST-server (15)
  connShutdown.score:  5.0
  connSetupTime.score:  3.5 (2)
  conn_setup_time:   0.000001000 (20)   0.000000000 (2)   2.000000000 (1)

Target 172.16.114.50       17 events
  from 1998-07-21 11:45:34.000403 EDT to 1998-07-21 12:43:26.000662 EDT
  from source estat-TCP-monitor
  clientAddr:  135.13.216.191
  server_port:  http (16)  smtp (1)
  connSetup.score:  5.0
  connShutdown.score:  5.0
  connSetupTime.score:  3.5 (1)
  conn_setup_time:   0.000001000 (9)   0.000000000 (7)
```

```
Target 172.16.114.50       14 events
  from 1998-07-21 12:09:21.000825 EDT to 1998-07-21 12:57:04.000332 EDT
  from source estat-TCP-monitor
  clientAddr:  194.7.248.153
  server_port:  http (13)  smtp (1)
  connSetup.score:  5.0
  conn_setup:  RST-server (1)
  connShutdown.score:  5.0
  connSetupTime.score:  3.5 (1)
  conn_setup_time:   0.000001000 (9)   0.000000000 (2)   2.000000000 (1)

Target 172.16.114.50       10 events
  from 1998-07-21 12:40:19.000237 EDT to 1998-07-21 16:14:21.000827 EDT
  from source estat-TCP-monitor
  clientAddr:  196.227.33.189
  server_port:  http (9)  smtp (1)
  connSetup.score:  5.0
  conn_setup:  RST-server (9)
  connShutdown.score:  5.0
  conn_setup_time:   0.000001000 (9)

Target 172.16.114.50       17 events
  from 1998-07-21 12:40:58.000135 EDT to 1998-07-21 17:18:14.000858 EDT
  from source estat-TCP-monitor
  clientAddr:  195.73.151.50
  server_port:  http (15)  smtp (2)
  connSetup.score:  5.0
  conn_setup:  RST-server (14)
  connShutdown.score:  5.0
  connSetupTime.score:  3.5 (1)
  conn_setup_time:   0.000001000 (11)   2.000000000 (1)

Target 172.16.114.50       16 events
  from 1998-07-21 13:48:54.000745 EDT to 1998-07-21 16:59:59.000510 EDT
  from source estat-TCP-monitor
  clientAddr:  195.115.218.108
  server_port:  http (13)  smtp (3)
  connSetup.score:  5.0
  conn_setup:  RST-server
  connShutdown.score:  5.0
  conn_setup_time:   0.000001000 (2)

Target 172.16.114.50       36 events
  from 1998-07-21 14:42:00.000519 EDT to 1998-07-21 18:41:38.000724 EDT
  from source estat-TCP-monitor
  clientAddr:  197.218.177.69
  server_port:  http
  connSetup.score:  5.0
  conn_setup:  RST-server
  connShutdown.score:  5.0
  conn_setup_time:   0.000001000 (20)   0.000000000 (8)
```

The following is a neptune attack against zeno (172.16.113.50) that indiscriminately flooded all low-numbered ports with about 200 connection requests each. Thus, a large number of requests resulted in reset-by-server (i.e., rejected request) events because the target port had no active service. A significant, but small relative to the total volume, number of the events went unanswered, indicating that the attack may have successfully overflowed the connection table. Also unusual was the number of connection requests reset by the client, suggesting that perhaps the client address was spoofed. There were no real victims of this attack (i.e., clients who persistently tried to access the service and were unsuccessful).

```
Target 172.16.113.50   199464 events
  from 1998-07-21 18:15:58.000307 EDT to 1998-07-21 19:07:55.000233 EDT
  from source estat-TCP-monitor
  clientAddr:  166.102.114.43
  server_port:  556 (200)  4 (200)  5 (200)  300 (200)
      Cutoff of 997 reached (200); remaining 1020 fields suppressed
        829 fields with 192 to 207 hits each suppressed
        141 fields with 176 to 191 hits each suppressed
         30 fields with 160 to 175 hits each suppressed
          6 fields with 144 to 159 hits each suppressed
          6 fields with 112 to 143 hits each suppressed
          5 fields with  96 to 111 hits each suppressed
          2 fields with  80 to  95 hits each suppressed
  connSetup.score:  5.0
  conn_setup:  RST-server (192132)  TO-server (1330)  RST-client (745)
  connSetupTime.score:  5.0 (199454)  4.5 (10)
  conn_setup_time:   0.000001000 (164749)   0.000000000 (20420)
    120.000000000 (854)  90.000000000 (337)   0.500000000 (32)
```

Some sample test result score plots:

- pascal
- zeno
- marx

Week 1 Friday:

The following is another neptune attack, this time against pascal (172.16.112.50). This attack was targeted specifically at four active ports: telnet, http, ftp-data, and finger, each getting around 200 connection requests, most of which went unanswered, implying that the attack successfully overflowed the connection table. There were no real victims of this attack (i.e., clients who persistently tried to access the service and were unsuccessful).

```
Target 172.16.112.50      790 events
  from 1998-07-24 14:41:32.000531 EDT to 1998-07-24 15:28:03.000096 EDT
  from source estat-TCP-monitor
  clientAddr:  9.9.9.9
  connPort.score:  3.5
  server_port:  telnet (199)  http (198)  ftp-data (198)  finger (195)
  connSetup.score:  5.0 (789)  3.0 (1)
  conn_setup:  TO-server (773)
  connShutdown.score:  5.0 (315)  3.5 (160)  3.0 (80)  4.5 (77)
  connSetupTime.score:  5.0 (787)  4.5 (1)
  conn_setup_time:  120.000000000 (295)  90.000000000 (116)
  connDuration.score:  3.0 (355)  4.0 (160)  5.0 (117)  3.5 (80)
```

The following report identifies a process-table attack against pascal (172.16.112.50). It is caught because many telnet sessions were used to mount the attack, each connection of which was improperly terminated, presumably due to downing the host or service. Because of the neptune attack that follows, it is hard for the statistical analyzer to determine an appropriate ending time for this attack.

```
Target 172.16.112.50      428 events
  from 1998-07-24 19:20:35.000597 EDT to 1998-07-24 21:37:44.000258 EDT
  from source estat-TCP-monitor
  clientAddr:  192.168.1.10
  connPort.score:  3.5 (390)  3.0 (38)
  server_port:  telnet
  connSetup.score:  5.0 (38)
  conn_setup:  OK (193)
  connShutdown.score:  5.0 (394)
  conn_shutdown:  TO-close (124)
  connSetupTime.score:  5.0 (38)
  conn_setup_time:   0.000001000 (94)   0.000000000 (27)   5.000000000 (1)
  connDuration.score:  5.0
  conn_duration:  240.000000000 (51)  900.000000000 (29)
    480.000000000 (22)
```

A neptune attack against pascal (172.16.112.50) indiscriminately bombarding low-numbered ports.

```
Target 172.16.112.50   204104 events
  from 1998-07-24 19:51:53.000397 EDT to 1998-07-24 20:42:52.000731 EDT
  from source estat-TCP-monitor
  clientAddr:  10.20.30.40
  connPort.score:  3.0 (114669)  3.5 (89435)
  server_port:  68 (200)  7 (200)  39 (200)  47 (200)
      Cutoff of 1020 reached (200); remaining 1017 fields suppressed
        1017 fields with 192 to 207 hits each suppressed
  connSetup.score:  5.0 (204102)  4.0 (1)
  conn_setup:  TO-server
  connShutdown.score:  5.0
  connSetupTime.score:  5.0 (204102)  4.5 (1)
  conn_setup_time:  120.000000000 (54285)  90.000000000 (32926)
    60.000000000 (17213)  900.000000000 (5068)  480.000000000 (1030)
  connDuration.score:  5.0
```

Sample test result score plots for pascal.

Week 2 Monday:

A saint (port scan) attack against pascal (172.16.112.50).

```
Target 172.16.112.50     3829 events
  from 1998-07-27 11:01:23.000596 EDT to 1998-07-27 11:03:57.000168 EDT
  from source estat-TCP-monitor
  clientAddr:  192.168.1.10
  connPort.score:  3.0 (3480)  3.5 (349)
  server_port:  4096 (1926)  8192 (1020)  0 (776)  cmd (4)
      Cutoff of 19 reached (2); remaining 102 fields suppressed
        102 fields with   0 to  15 hits each suppressed
  connSetup.score:  5.0 (3822)  3.0 (1)
  conn_setup:  RST-server (3493)  TO-server (253)
  connShutdown.score:  5.0 (3808)
  conn_shutdown:  RST-client (1)
  connSetupTime.score:  5.0 (400)  4.5 (5)  4.0 (1)  3.5 (1)
  conn_setup_time:   0.000000000 (1839)   0.000001000 (1516)
    120.000000000 (323)   2.000000000 (13)
  connDuration.score:  3.0 (1801)  5.0 (329)  3.5 (306)  4.0 (1)
  conn_duration:  10.000000000 (1)
```

A portsweep attack against pascal (172.16.112.50).

```
Target 172.16.112.50      276 events
  from 1998-07-27 14:01:29.000711 EDT to 1998-07-27 14:17:36.000159 EDT
  from source estat-TCP-monitor
  clientAddr:  202.247.224.89
  connPort.score:  3.5
  server_port:  624 (1)  185 (1)  308 (1)  67 (1)  326 (1)  242 (1)
    at-nbp (1)  598 (1)  700 (1)  256 (1)  693 (1)  107 (1)  96 (1)
    715 (1)  379 (1)  336 (1)  890 (1)  488 (1)  349 (1)  545 (1)  365 (1)
    629 (1)  320 (1)  466 (1)  407 (1)  671 (1)  949 (1)  37 (1)  825 (1)
    at-zis (1)  989 (1)  446 (1)  213 (1)  137 (1)  91 (1)  508 (1)
    203 (1)  431 (1)  896 (1)  410 (1)  607 (1)  483 (1)  471 (1)  130 (1)
    215 (1)  408 (1)  198 (1)  311 (1)  903 (1)  765 (1)  922 (1)  653 (1)
    56 (1)  590 (1)  181 (1)  288 (1)  425 (1)  793 (1)  361 (1)  768 (1)
    997 (1)  458 (1)  782 (1)  424 (1)  162 (1)  279 (1)  658 (1)  865 (1)
    321 (1)  342 (1)  888 (1)  523 (1)  866 (1)  120 (1)  350 (1)  207 (1)
    631 (1)  110 (1)  367 (1)  101 (1)  81 (1)  412 (1)  885 (1)  190 (1)
    280 (1)  691 (1)  245 (1)  781 (1)  0 (1)  928 (1)  261 (1)  998 (1)
    371 (1)  1017 (1)  15 (1)  324 (1)  383 (1)  39 (1)  726 (1)  163 (1)
    720 (1)  284 (1)  178 (1)  945 (1)  494 (1)  3 (1)  477 (1)  220 (1)
    676 (1)  75 (1)  30 (1)  900 (1)  665 (1)  747 (1)  156 (1)  332 (1)
    978 (1)  724 (1)  ftp-data (1)  977 (1)  217 (1)  1014 (1)  493 (1)
    277 (1)  186 (1)  944 (1)  14 (1)  416 (1)  554 (1)  619 (1)  736 (1)
    927 (1)  573 (1)  301 (1)  129 (1)  183 (1)  574 (1)  374 (1)  766 (1)
    208 (1)  484 (1)  441 (1)  138 (1)  729 (1)  892 (1)  38 (1)  4 (1)
    210 (1)  962 (1)  774 (1)  586 (1)  968 (1)  31 (1)  118 (1)  278 (1)
    969 (1)  430 (1)  169 (1)  862 (1)  633 (1)  317 (1)  420 (1)  1006 (1)
    681 (1)  474 (1)  918 (1)  cmd (1)  141 (1)  1019 (1)  634 (1)  319 (1)
    839 (1)  148 (1)  376 (1)  612 (1)  856 (1)  281 (1)  17 (1)  829 (1)
    102 (1)  19 (1)  843 (1)  1011 (1)  814 (1)  576 (1)  852 (1)  531 (1)
    522 (1)  529 (1)  698 (1)  180 (1)  929 (1)  785 (1)  451 (1)  925 (1)
    111 (1)  636 (1)  547 (1)  543 (1)  1012 (1)  114 (1)  487 (1)  622 (1)
    727 (1)  864 (1)  641 (1)  745 (1)  515 (1)  337 (1)  687 (1)  538 (1)
    355 (1)  580 (1)  357 (1)  842 (1)  1021 (1)  296 (1)  719 (1)  195 (1)
    218 (1)  911 (1)  434 (1)  679 (1)  399 (1)  670 (1)  877 (1)  965 (1)
    587 (1)  338 (1)  1 (1)  840 (1)  915 (1)  128 (1)  52 (1)  646 (1)
    897 (1)  263 (1)  254 (1)  428 (1)  751 (1)  476 (1)  966 (1)  692 (1)
    389 (1)  733 (1)  826 (1)  450 (1)  933 (1)  480 (1)  27 (1)  418 (1)
    179 (1)  626 (1)  176 (1)  754 (1)  57 (1)  89 (1)  555 (1)  375 (1)
    457 (1)  556 (1)  502 (1)  798 (1)  648 (1)  359 (1)  249 (1)  859 (1)
    268 (1)  718 (1)  151 (1)  678 (1)  820 (1)  468 (1)  93 (1)  373 (1)
    398 (1)
  connSetup.score:  5.0
  conn_setup:  RST-server (250)
  connSetupTime.score:  3.5 (1)
  conn_setup_time:  0.000001000 (188)  0.000000000 (30)
    120.000000000 (4)
  connDuration.score:  4.5 (274)  4.0 (2)
```

An apache2 http attack against marx (172.16.114.50).

```
Target 172.16.114.50      183 events
  from 1998-07-27 18:36:26.000316 EDT to 1998-07-27 18:39:41.000751 EDT
  from source estat-TCP-monitor
  clientAddr:  196.227.33.189
  server_port:  http
  connSetup.score:  5.0
  connShutdown.score:  5.0
  conn_shutdown:  RST-server (180)
  connSetupTime.score:  3.5
  conn_duration:  900.000000000 (140)  480.000000000 (38)
```

The following "detections" are on data for this day after the time-stamp data became corrupted in the LL dataset (note the date in the time-stamps leaped ahead by 3 days) and are therefore not being counted as either detections or false alerts.

```
Target 172.16.112.50      245 events
  from 1998-07-30 22:59:07.000240 EDT to 1998-07-30 23:01:25.000121 EDT
  from source estat-TCP-monitor
  clientAddr:  1.2.3.4
  connPort.score:  3.5
  server_port:  telnet (140)  http (105)
  connSetup.score:  5.0
  conn_setup:  TO-server
  connShutdown.score:  3.0 (240)  5.0 (5)
  connSetupTime.score:  5.0
  conn_setup_time:  120.000000000 (37)  90.000000000 (34)
    900.000000000 (32)  480.000000000 (17)
  connDuration.score:  5.0

Target 172.16.112.20       23 events
  from 1998-07-30 23:16:11.000294 EDT to 1998-07-30 23:16:25.000179 EDT
  from source estat-TCP-monitor
  clientAddr:  192.168.1.10
  connPort.score:  4.5 (11)  3.5 (1)
  server_port:  telnet (7)  143 (4)  53 (4)  110 (4)  finger (3)  http (1)
  connSetup.score:  5.0 (22)
  conn_setup:  OK (1)  RST-server (1)
  connShutdown.score:  5.0 (15)
  conn_shutdown:  RST-client (5)  OK (2)
  connSetupTime.score:  4.0 (6)  5.0 (4)
  conn_setup_time:   0.000001000 (7)   0.000000000 (2)
  connDuration.score:  5.0
```

Week 2 Tuesday:

This corresponds to a guest attack in the LL list file, presumably trying to guess an FTP account. These are caught only because the connection shutdown was client-reset and the duration was unusual (i.e., there is very little information provided in this report to deduce that it was a guest attack and not some other failure).

```
Target 172.16.112.50       52 events
  from 1998-07-28 11:20:57.000940 EDT to 1998-07-28 15:24:23.000423 EDT
  from source estat-TCP-monitor
  clientAddr:  195.73.151.50
  connPort.score:  3.5
  server_port:  ftp
  conn_setup:  OK (18)
  connShutdown.score:  5.0
  conn_shutdown:  RST-client (34)
  connSetupTime.score:  5.0 (32)  4.0 (6)  3.5 (5)  4.5 (4)
  conn_setup_time:   0.000001000 (10)   0.500000000 (1)
  connDuration.score:  5.0 (48)  4.5 (3)  3.0 (1)
  conn_duration:   0.000010000 (1)
```

A satan (port scan) attack against zeno.

```
Target 172.16.113.50     8986 events
  from 1998-07-28 15:17:29.000287 EDT to 1998-07-28 15:18:31.000707 EDT
  from source estat-TCP-monitor
  clientAddr:  208.253.77.185
  server_port:  4096 (3715)  0 (2654)  8192 (1709)  telnet (2)
      Cutoff of 44 reached (2); remaining 898 fields suppressed
        898 fields with   0 to  15 hits each suppressed
  connSetup.score:  5.0
  conn_setup:  RST-server (8593)  TO-server (273)
  connShutdown.score:  5.0 (5411)  4.0 (2188)  3.0 (1)
  conn_shutdown:  OK (4)  RST-server (1)  RST-client (1)
  connSetupTime.score:  5.0 (8927)  4.5 (10)  4.0 (10)  3.5 (6)  3.0 (4)
  conn_setup_time:   0.000001000 (4086)  120.000000000 (298)
     2.000000000 (281)   0.500000000 (42)
  connDuration.score:  3.5 (6421)  3.0 (901)
  conn_duration:   1.000000000 (6)   5.000000000 (2)   0.100000000 (1)
     0.000010000 (1)
```

The following 12 attack reports are for an mscan attack against several hosts (one attack report each).

```
Target 172.16.112.20      171 events
  from 1998-07-28 17:36:28.000720 EDT to 1998-07-29 02:48:56.000493 EDT
  from source estat-TCP-monitor
  clientAddr:  207.75.239.115
  connPort.score:  4.5 (125)  4.0 (4)  3.0 (2)  3.5 (1)
  server_port:  telnet (99)  110 (48)  143 (22)  53 (1)  111 (1)
  connSetup.score:  5.0 (167)
  conn_setup:  RST-server (34)  OK (2)
  connShutdown.score:  5.0 (169)
  conn_shutdown:  RST-client (91)  OK (1)
  connSetupTime.score:  5.0 (37)  3.0 (1)
  conn_setup_time:   0.000001000 (26)   0.000000000 (21)
  connDuration.score:  5.0 (169)  4.5 (2)
  conn_duration:   1.000000000 (11)   0.000010000 (1)

Target 172.16.112.207      91 events
  from 1998-07-28 17:36:29.000700 EDT to 1998-07-29 02:48:58.000393 EDT
  from source estat-TCP-monitor
  clientAddr:  207.75.239.115
  server_port:  telnet (63)  110 (19)  143 (8)  111 (1)
  connSetup.score:  4.0 (90)
  conn_setup:  OK (14)  RST-server (11)
  connShutdown.score:  5.0
  conn_shutdown:  RST-client (33)
  connSetupTime.score:  3.5 (3)
  conn_setup_time:   0.000001000 (2)   2.000000000 (1)
  connDuration.score:  3.0 (79)
  conn_duration:   1.000000000 (2)   0.000010000 (2)  240.000000000 (1)

Target 172.16.112.194     100 events
  from 1998-07-28 17:36:32.000035 EDT to 1998-07-29 02:49:01.000190 EDT
  from source estat-TCP-monitor
  clientAddr:  207.75.239.115
  server_port:  111 (30)  143 (27)  110 (23)  telnet (20)
  connSetup.score:  4.0 (97)
  conn_setup:  RST-server (27)  OK (7)
  connShutdown.score:  5.0
  conn_shutdown:  RST-client (14)  OK (8)
  conn_setup_time:   0.000001000 (16)   0.000000000 (16)
  conn_duration:   1.000000000 (15)

Target 172.16.113.84       191 events
  from 1998-07-28 17:36:32.000978 EDT to 1998-07-29 02:49:00.000400 EDT
  from source estat-TCP-monitor
  clientAddr:  207.75.239.115
  server_port:  telnet (66)  110 (51)  143 (49)  111 (25)
  connSetup.score:  4.0
  conn_setup:  OK (51)  RST-server (25)
  connShutdown.score:  4.0
  conn_shutdown:  RST-client (50)
  conn_setup_time:   0.000001000 (49)   0.000000000 (27)
  connDuration.score:  3.0 (149)
  conn_duration:   1.000000000 (32)

Target 172.16.112.50        59 events
  from 1998-07-28 17:36:44.000355 EDT to 1998-07-29 02:49:17.000071 EDT
  from source estat-TCP-monitor
  clientAddr:  207.75.239.115
  connPort.score:  3.5
  server_port:  telnet (37)  143 (18)  110 (3)  ftp (1)
  connSetup.score:  5.0 (58)
  conn_setup:  RST-server (21)  OK (1)
  connShutdown.score:  5.0 (53)  4.5 (3)
  conn_shutdown:  RST-client (6)
  connSetupTime.score:  5.0 (36)  4.5 (3)  4.0 (1)  3.0 (1)
  conn_setup_time:   0.000001000 (13)   0.000000000 (4)
  connDuration.score:  5.0 (54)  4.5 (3)  3.5 (2)
  conn_duration:   0.000010000 (1)   1.000000000 (1)

Target 172.16.113.50        84 events
  from 1998-07-28 17:36:44.000359 EDT to 1998-07-29 02:49:16.000857 EDT
  from source estat-TCP-monitor
  clientAddr:  207.75.239.115
  server_port:  telnet (69)  110 (15)
  connSetup.score:  5.0
  conn_setup:  OK (35)
  connShutdown.score:  5.0 (83)  4.5 (1)
  conn_shutdown:  OK (12)  RST-client (1)
  connSetupTime.score:  4.0 (1)
  conn_setup_time:   0.000001000 (26)   2.000000000 (1)
  connDuration.score:  3.5 (5)  3.0 (3)
  conn_duration:   0.000010000 (8)   0.100000000 (3)   1.000000000 (1)

Target 172.16.114.168      133 events
  from 1998-07-28 17:36:47.000171 EDT to 1998-07-29 02:49:09.000720 EDT
  from source estat-TCP-monitor
  clientAddr:  207.75.239.115
  server_port:  143 (42)  110 (42)  111 (26)  telnet (23)
  connSetup.score:  4.0
  conn_setup:  OK (28)  RST-server (22)
  connShutdown.score:  4.0
  conn_shutdown:  RST-client (27)  OK (11)
  conn_setup_time:   0.000000000 (49)   0.000001000 (33)
  conn_duration:   5.000000000 (4)   1.000000000 (2)

Target 172.16.113.105      93 events
  from 1998-07-28 17:36:48.000347 EDT to 1998-07-29 02:49:10.000929 EDT
  from source estat-TCP-monitor
  clientAddr:  207.75.239.115
  server_port:  telnet (58)  110 (18)  143 (17)
  connSetup.score:  4.0
  conn_setup:  OK (20)  RST-server (19)
  connShutdown.score:  5.0
  conn_shutdown:  RST-client (45)
  conn_setup_time:   0.000001000 (21)   0.000000000 (8)
  connDuration.score:  3.0 (53)
  conn_duration:   1.000000000 (8)   0.000010000 (5)   0.100000000 (2)

Target 172.16.112.149      83 events
  from 1998-07-28 17:36:48.000814 EDT to 1998-07-29 02:49:13.000128 EDT
  from source estat-TCP-monitor
  clientAddr:  207.75.239.115
  server_port:  telnet (55)  110 (19)  143 (9)
  connSetup.score:  4.0
  conn_setup:  RST-server (24)  OK (3)
  connShutdown.score:  5.0
  conn_shutdown:  RST-client (24)
  conn_setup_time:   0.000001000 (20)   0.000000000 (6)
  connDuration.score:  3.0 (75)
  conn_duration:   1.000000000 (5)

Target 172.16.114.207      94 events
  from 1998-07-28 17:36:49.000164 EDT to 1998-07-29 02:49:13.000871 EDT
  from source estat-TCP-monitor
  clientAddr:  207.75.239.115
  server_port:  telnet (56)  110 (22)  143 (13)  111 (3)
  connSetup.score:  4.0
  conn_setup:  OK (35)  RST-server (15)
  connShutdown.score:  5.0
  conn_shutdown:  RST-client (38)
  conn_setup_time:   0.000001000 (37)   0.000000000 (17)
  conn_duration:   1.000000000 (10)   0.000010000 (6)

Target 172.16.114.169      125 events
  from 1998-07-28 17:36:46.000002 EDT to 1998-07-29 02:20:20.000540 EDT
  from source estat-TCP-monitor
  clientAddr:  207.75.239.115
  server_port:  telnet (42)  110 (34)  143 (32)  111 (17)
  connSetup.score:  4.0
  conn_setup:  RST-server (34)  OK (6)
  connShutdown.score:  4.0
  conn_shutdown:  RST-client (22)  TO-close (2)
  conn_setup_time:   0.000001000 (1)
  connDuration.score:  3.0 (106)
  conn_duration:   1.000000000 (5)  240.000000000 (2)

Target 172.16.113.204      95 events
  from 1998-07-28 18:04:57.000204 EDT to 1998-07-29 02:49:11.000945 EDT
  from source estat-TCP-monitor
  clientAddr:  207.75.239.115
  server_port:  telnet (71)  110 (15)  143 (9)
  connSetup.score:  4.0
  conn_setup:  OK (32)  RST-server (19)
  connShutdown.score:  4.0
  conn_shutdown:  RST-client (34)
  conn_setup_time:   0.000001000 (26)   0.000000000 (9)
  connDuration.score:  3.0 (32)  3.5 (22)
  conn_duration:  1.000000000 (7)   0.100000000 (6)   5.000000000 (4)
```

A processtable attack against pascal (172.16.112.50).

```
Target 172.16.112.50      265 events
  from 1998-07-28 18:04:59.000965 EDT to 1998-07-28 20:21:20.000640 EDT
  from source estat-TCP-monitor
  clientAddr:  192.168.1.10
  connPort.score:  3.5
  server_port:  telnet
  connSetup.score:  5.0 (117)  3.5 (29)
  conn_setup:  OK (10)
  connShutdown.score:  5.0 (232)
  conn_shutdown:  TO-close (115)  OK (11)
  connSetupTime.score:  4.5 (36)
  conn_setup_time:   0.000001000 (23)   0.000000000 (2)   0.500000000 (1)
  connDuration.score:  5.0 (250)  4.0 (15)
  conn_duration:  240.000000000 (44)
```

Week 2 Wednesday:

A (comparatively lightweight) neptune attack against zeno's telnet port.

```
Target 172.16.113.50      97 events
  from 1998-07-29 11:11:30.000534 EDT to 1998-07-29 11:11:30.000854 EDT
  from source estat-TCP-monitor
  clientAddr:  10.140.175.64
  server_port:  telnet
  connSetup.score:  5.0
  conn_setup:  TO-server
  connSetupTime.score:  5.0
  conn_setup_time:  120.000000000
```

An xlock attack. The reasons for detecting this attack are admittedly unclear from this report. We suspect that the high measure scores are due, in part, to residual effects from the prior warez and/or ps attacks (not detected). This, combined with the connection shutdown measure scoring high, implies that there were several other clients whose connections were adversely impacted, but who did not generate sufficient traffic to create victim reports.

```
Target 172.16.112.50      10 events
  from 1998-07-29 14:10:49.000099 EDT to 1998-07-29 23:49:31.000206 EDT
  from source estat-TCP-monitor
  clientAddr:  197.218.177.69
  connPort.score:  3.5
  server_port:  6000 (4)  ftp (4)  telnet (2)
  conn_setup:  OK (5)
  connShutdown.score:  5.0 (1)
  conn_shutdown:  OK (4)  TO (1)
  connSetupTime.score:  5.0
  connDuration.score:  5.0
```

Week 2 Thursday:

A blanket neptune attack against zeno's low-numbered ports.

```
Target 172.16.113.50   197788 events
  from 1998-07-30 13:30:50.000369 EDT to 1998-07-30 14:23:03.000695 EDT
  from source estat-TCP-monitor
  clientAddr:  209.74.60.168
  server_port:  326 (200)  517 (200)  518 (200)  306 (200)
      Cutoff of 988 reached (200); remaining 1020 fields suppressed
        754 fields with 192 to 207 hits each suppressed
        211 fields with 176 to 191 hits each suppressed
         34 fields with 160 to 175 hits each suppressed
          9 fields with 144 to 159 hits each suppressed
          9 fields with 128 to 143 hits each suppressed
          2 fields with  80 to 111 hits each suppressed
  connSetup.score:  5.0
  conn_setup:  RST-server (188054)  TO-server (2653)  RST-client (872)
  connSetupTime.score:  5.0 (197517)  4.5 (209)  4.0 (62)
  conn_setup_time:   0.000001000 (155767)   0.000000000 (16798)
    120.000000000 (2329)  60.000000000 (205)  90.000000000 (171)
     0.000100000 (72)   0.500000000 (19)
```

Another processtable attack against pascal.

```
Target 172.16.112.50      263 events
  from 1998-07-30 18:00:03.000635 EDT to 1998-07-30 20:13:48.000080 EDT
  from source estat-TCP-monitor
  clientAddr:  192.168.1.10
  connPort.score:  3.5
  server_port:  telnet
  connSetup.score:  5.0 (22)
  conn_setup:  OK (22)
  connShutdown.score:  5.0 (243)
  conn_shutdown:  TO-close (200)  OK (20)
  connSetupTime.score:  5.0 (20)
  conn_setup_time:   0.000001000 (8)   0.000000000 (1)   2.000000000 (1)
  connDuration.score:  5.0
  conn_duration:  240.000000000 (115)
```

A port-targeted neptune attack against pascal.

```
Target 172.16.112.50      508 events
  from 1998-07-30 20:15:14.000834 EDT to 1998-07-30 21:01:02.000763 EDT
  from source estat-TCP-monitor
  clientAddr:  135.13.216.191
  connPort.score:  3.5
  server_port:  ftp-data (139)  telnet (138)  finger (125)  http (106)
  connSetup.score:  5.0
  conn_setup:  RST-client (181)  RST-server (80)
  connShutdown.score:  5.0 (505)
  connSetupTime.score:  5.0 (1)
  conn_setup_time:   0.000001000 (159)   0.000000000 (119)
     0.500000000 (1)
  connDuration.score:  5.0
```

A side-effect of the mail-bomb attack and perhaps piggy-back influence.

```
Target 172.16.112.50       22 events
  from 1998-07-30 22:08:01.000381 EDT to 1998-07-30 22:08:13.000965 EDT
  from source estat-TCP-monitor
  clientAddr:  204.233.47.21
  connPort.score:  3.5
  server_port:  smtp
  conn_setup:  OK (11)
  connShutdown.score:  5.0
  conn_setup_time:   0.000000000 (8)   0.000001000 (3)
  connDuration.score:  5.0
  conn_duration:   1.000000000 (9)
```

Week 2 Friday:

A saint attack.

```
Target 172.16.112.20       17 events
  from 1998-07-31 10:22:48.000210 EDT to 1998-07-31 10:23:17.000960 EDT
  from source estat-TCP-monitor
  clientAddr:  197.218.177.69
  server_port:  finger (12)  ftp (1)  telnet (1)  gopher (1)  6000 (1)
    smtp (1)
  connSetup.score:  5.0
  conn_shutdown:  OK (11)
  conn_setup_time:   0.000001000 (5)   0.000000000 (1)
  connDuration.score:  5.0 (16)  3.0 (1)
  conn_duration:   1.000000000 (5)   0.100000000 (1)
```

A neptune attack.

```
Target 172.16.112.50     1000 events
  from 1998-07-31 10:30:31.000233 EDT to 1998-07-31 10:30:31.000463 EDT
  from source estat-TCP-monitor
  clientAddr:  18.28.38.48
  connPort.score:  3.5
  server_port:  telnet
  connSetup.score:  5.0
  conn_setup:  TO-server (920)
  connSetupTime.score:  5.0 (999)  3.5 (1)
  conn_setup_time:  90.000000000 (965)  60.000000000 (21)
  connDuration.score:  5.0
```

An apache2 attack.

```
Target 172.16.114.50      150 events
  from 1998-07-31 21:39:09.000629 EDT to 1998-07-31 21:40:16.000912 EDT
  from source estat-TCP-monitor
  clientAddr:  202.72.1.77
  server_port:  http
  connSetup.score:  5.0
  connShutdown.score:  5.0 (149)  4.5 (1)
  conn_shutdown:  RST-server (142)
  connSetupTime.score:  3.5
  conn_duration:  1800.000000000 (149)
```

Last modified: Fri Jul 9 10:31:24 PDT 1999